UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	*	
	*	
v.	*	Criminal No. 17-cr-10066-IT
	*	
FERNANDO RIVERA RODRIGUEZ,	*	
YEURYS TEJEDA, JOSE NEGRON,	*	
and ISIS Y LUGO-GUERRERO,	*	
	*	
Defendants.	*	

MEMORANDUM & ORDER

February 20, 2018

TALWANI, D.J.

This case involves a prosecution based largely on evidence derived from government interception of wire and electronic communications. Presently before the court is the Motion to Suppress Evidence Derived from Electronic Surveillance Where Wiretap Order was Insufficient on its Face [#253] filed by Defendant Fernando Rivera Rodriguez,[1] and joined by Defendants Isis Lugo-Guerrero and Jose Negron,[2] and Defendant Yeurys Tejeda's Motion to Suppress Evidence Derived from Wiretap Orders [#282], which incorporates the legal arguments made in Rivera Rodriguez's motion. For the reasons that follow, the suppression motions are DENIED.

I. Title III's Landscape

Defendants bring their suppression motions pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, see 18 U.S.C. §§ 2510-2522. This statute "authorized

[1] Fernando Rivera Rodriguez is also known by his real name, Jose Antonio Lugo-Guerrero.

[2] The court allowed these Defendants' motions to join in Rivera Rodriguez's Motion to Suppress. See Electronic Order [#300], allowing Motions for Joinder [#255, #299].

wiretapping as needed to allow effective investigation of criminal activities while at the same time ensuring meaningful judicial supervision and requiring specific procedures to safeguard privacy rights." United States v. Gordon, 871 F.3d 35, 43 (1st Cir. 2017).

Law enforcement officers seeking authorization to intercept communications must apply to a "judge of competent jurisdiction." 18 U.S.C. § 2518(1). Each application must contain certain information, including "the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application." Id. § 2518(1)(a). Another section of the statute governing the authorization process provides that only certain officials in the Department of Justice may authorize federal wiretap applications. See id. § 2516(1).

Upon reviewing such an application, "the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications," so long as the judge is satisfied that the applicant has met the application requirements. Id. § 2518(3). Each order authorizing or approving interception must contain certain information. Id. § 2518(4). Relevant here, it must specify "the identity of the agency authorized to intercept the communications, and of the person authorizing the application." Id. § 2518(4)(d). Section 2518(4) provides further that an authorization order "shall, upon request of the applicant, direct that a provider of wire or electronic communication service . . . shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference." "Applications made and orders granted under . . . [Title III] shall be sealed by the judge," and "shall be disclosed only upon a showing of good cause." Id. § 2518(8)(b).

An "aggrieved person in any trial, hearing, or proceeding in or before any court . . . may move to suppress the contents of any wire or oral communication intercepted pursuant

to . . . [Title III], or evidence derived therefrom," id. § 2518(10)(a), if, as relevant here, "the order of authorization or approval under which [the communication] was intercepted is insufficient on its face." Id. § 2518(10)(a)(ii).[3] An "aggrieved person" is a "person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed." Id. § 2510(11).

II. Factual Background

A federal district judge in the District of Massachusetts issued on June 22, 2016, a sealed order authorizing the Drug Enforcement Administration ("DEA") to intercept communications made from two target telephone numbers. Along with providing other information required by Title III, the order named an Acting Deputy Assistant Attorney General in the Department of Justice who was a duly designated official of the Criminal Division for authorizing wiretap applications as the official who authorized the application. It also provided that, "based upon the request of the Applicant," a service provider was to "furnish and continue to furnish the Applicant and DEA with all information, facilities, and technical assistance necessary to accomplish the interceptions unobtrusively and with a minimum of interference." Further, the authorization order stated, "this Order, any resulting Orders, and all interim reports filed with the Court with regard to this matter shall be SEALED until further order of the Court, except that copies of the Order, in full or redacted form, may be provided to the Applicant and may be served on the communication service provider as necessary to effectuate the Court's Orders."[4]

[3] Suppression may also be warranted if "(i) the communication was unlawfully intercepted; [or] . . . (iii) the interception was not made in conformity with the order of authorization or approval." Id. § 2518(10)(a). Defendants rely solely on § 2518(10)(a)(ii) as a basis for suppression.

[4] The authorization orders were not filed on this case's docket but were reviewed by the court in connection with the motions to suppress. Counsel for the Defendants confirmed at the hearing on the motions that the government had provided them copies of these authorization orders.

On the same day that it issued the above authorization order, the court issued what it labeled a "Service Provider Order." See Sealed Docket Entry [#277-1] ("June 22 service provider order"). This June 22 service provider order stated that the government had applied for an order authorizing the interception of wire communications, and that "[t]he Court, having previously reviewed the Application and found that it conforms in all respects to the requirements of [Title III], has this day signed an Order conforming to the provisions of [Title III], authorizing the Drug Enforcement Administration (DEA) to conduct the aforesaid interceptions." Id. The June 22 service provider order ordered, *inter alia*, that: (1) the service provider would furnish the DEA with information, facilities, and technical assistance to accomplish the interceptions; (2) the DEA would compensate the service provider; (3) the service provider's assistance would terminate in thirty days; and (4) the DEA could use specified practices to intercept the communications. Id. Finally, the June 22 service provider order stated "this Order is SEALED." Id. The district judge signed and dated the service provider order. Id.

The government subsequently sought authorization to intercept additional wire communications. An authorization order and a separate service provider order were issued on July 29. Again, the authorization order named a Deputy Assistant Attorney General in the Department of Justice who was a duly designated official of the Criminal Division for authorizing wiretap applications as the official who authorized the application for interception of communications, and again the authorization order provided that, based upon the "request of the Applicant," a service provider was to "furnish and continue to furnish the Applicant and DEA with all information, facilities, and technical assistance necessary to accomplish the interceptions unobtrusively and with a minimum of interference." Sealed Docket Entry [#277-2] ("July 29 service provider order"). Although similar to the June 22 service provider order, the July 29

service provider order did not refer to a separate order approved by the court and concluded by stating "this Order, any resulting Orders, and all interim reports filed with the Court with regard to this matter shall be SEALED until further order of the Court, except that copies of the Order, in full or redacted form, may be provided to the Applicant and may be served on the communication service provider as necessary to effectuate the Court's Orders." Id.

The court continued to follow this process of issuing separate authorization and service provider orders as the investigation progressed. Authorization orders were issued on October 18, 2016, December 9, 2016, and January 26, 2017. Each authorization order named either a Deputy Assistant Attorney General or Acting Assistant Attorney General in the Department of Justice who was a duly designated official of the Criminal Division for authorizing wiretap applications as the official who authorized the application for interception of communications, and provided that a service provider was to "furnish and continue to furnish the Applicant and DEA with all information, facilities, and technical assistance necessary to accomplish the interceptions unobtrusively and with a minimum of interference." Each concluded by stating "that copies of the Order, in full or redacted form, may be provided to the Applicant and may be served on the communication service provider as necessary to effectuate the Court's Orders." Service provider orders were issued on the same dates as the authorization orders. These three service provider orders were similar to the July 29 service provider order, although they did not contain the provision stating that the orders would be sealed until further court order and that copies of the orders could be provided to the applicant and served on the service provider as necessary.

III. Discussion

At issue is whether the orders that went to the service providers were facially insufficient orders authorizing interception of their communications and, if so, whether this insufficiency

warrants suppression. Defendants do not dispute that a qualified official in the Department of Justice authorized the wiretap applications, that the wiretap applications complied with Title III, or that the authorization orders approving the wiretap applications and providing that a service provider was to furnish and continue to furnish the Applicant and DEA with all information, facilities, and technical assistance necessary to accomplish the interceptions complied with Title III. Their sole argument is that the derivative *service provider orders* did not provide the "identity of . . . the person authorizing the application." 18 U.S.C. § 2518(4). This presents a pure question of law as to whether these derivative orders are themselves subject to the requirements of § 2518(4).

Defendants rely on the statutory language and United States v. Scurry, 821 F.3d 1 (D.C. Cir. 2016). Scurry held that authorization orders that failed to identify authorizing officials by name were "facially insufficient" pursuant to § 2518(10)(a)(ii), and thus subject to suppression. Id. at 6. In Scurry, the authorization orders – the only orders at issue in that case – failed to include "the identity . . . of the person authorizing the application." Id. at 8 (quoting § 2518(4)(d)). Only asterisks appeared in place of the authorizing official's name. Id. In holding that the authorization orders at issue were facially insufficient despite the valid applications, Scurry rejected the government's argument that inclusion of an authorizing official's identity in an application cured the omission of that official's identity from the court's order authorizing the wiretap. Id. at 9.

The First Circuit has not yet adopted the D.C. Circuit's approach in Scurry. Even if it were to do so, however, the facts presented in Scurry are readily distinguishable from those presented here. Scurry did not involve derivative service provider orders. In this case, unlike in Scurry, the court issued authorization orders that fully complied with the requirements of

§ 2518(4). Therefore, Scurry's holding that a complete authorization order is required does not resolve the issue. There is no dispute in this case that each of the authorization orders issued by the district judge contained the information that Title III requires.

Title III does not refer to derivative service provider orders,[5] but Defendants urge the court to rely on Scurry to conclude that the requirement of identifying the official authorizing the application must apply to any such orders as well. In concluding Title III intended the authorizing official's identity to appear in both the application and authorization order, as Title III's text provides, Scurry reasoned that the purpose of the duplicative requirement was that "[a]fter the authorizing judge signs the wiretap order, the order – but not the application – goes to those involved in conducting the surveillance." 821 F.3d at 10. Scurry noted that the identification requirement in the application "facilitates the court's ability to conclude that the application has been properly approved." Id. at 11 (quoting United States v. Chavez, 416 U.S. 562, 575 (1974)). Scurry concluded that the identification requirement "in the wiretap order facilitates additional oversight, this time by the parties executing the order." Id.

As to derivative orders to third-party providers designed to effectuate compliant authorization orders, Scurry is unpersuasive. Scurry cites no legal authority for its conclusion that Congress intended § 2518(4) to furnish service providers with the ability to provide additional oversight over interceptions. In Chavez, the Supreme Court concluded: "Requiring identification of the authorizing official in the application facilitates the *court*'s ability to

[5] A Department of Justice Manual outlining the Title III authorization process cites § 2518(4) for the proposition that, in addition to issuing an authorization order, a "court should also issue a technical assistance order to the communications provider." The Manual describes a service provider order as "a redacted order that requires the telephone company or other service provider to assist the agents in effecting the electronic surveillance." Electronic Surveillance – Title III Orders, Dep't of Justice Resource Manual Title 9 No. 30 (2018).

conclude that the application has been properly approved under § 2516; requiring identification in the court's order also serves to 'fix responsibility' for the source of preliminary approval." 416 U.S. at 575 (emphasis added). The Court then proceeded to state that another purpose of the dual identification requirements is to assist judges and the United States courts in compiling reports regarding actions taken on wiretap applications. Id. at 577. Citing to legislative history, the Court concluded that these reports then facilitate public evaluation of interceptions pursuant to Title III. Id. Finally, the Court observed that there was no legislative history to suggest that the dual identification requirements "were meant, by themselves, to occupy a central, or even functional, role in guarding against unwarranted use of wiretapping or electronic surveillance." Id. at 578. As to these requirements, "[n]o role more significant than a reporting function designed to establish on paper that one of the major procedural protections of Title III had been properly accomplished is apparent." Id. at 579.

Fixing responsibility, ensuring judicial scrutiny of Title III applications, aiding in reporting on Title III interceptions overall, and assisting in appellate review of Title III interceptions are all purposes served by the requirement that an authorization order provide the information listed in § 2518(4). None of these purposes, however, leads to the conclusion that Congress intended service providers to receive all of the information listed in § 2518(4). To hold to the contrary would mean that Title III also requires that every service provider who is ordered to assist in intercepting communications learn not only the authorizing official, but also *all* of the other information required by § 2518(4), including, for example, "a statement of the particular offense to which [a communication] relates," id. § 2518(4)(c), as well as "the identity of the person, if known, whose communications are to be intercepted," id. § 2518(4)(a).

It is for the court, and not the service provider, to decide whether interception is warranted. If a service provider fails to comply with an authorization order, the court can issue an enforcement order directing the provider to comply and imposing civil penalties for non-compliance. Id. §2522(c)(1). In turn, Title III immunizes service providers that comply with court orders. It states that a service provider is authorized by law to intercept communications if the provider "has been provided with – (A) a court order directing such assistance . . . setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required." Id. § 2511(2)(a)(ii). This section further provides that "[n]o cause of action shall lie in any court against any provider of wire or electronic communication service . . . for providing information, facilities, or assistance in accordance with the terms of a court order . . . under this chapter." Id. Further, Title III provides a complete defense against any civil or criminal actions for "good faith reliance on – (1) a court . . . order." Id. § 2520(d).

Ultimately, the court finds no support for Defendants' contention that the derivative orders at issue here needed to conform to the requirements of § 2518(4). These derivative orders effectuated the court's authorization orders by informing service providers that they had been ordered to facilitate interception of certain communications. The underlying "order[s] authorizing or approving" such interception fully complied with § 2518(4). Defendants have not shown that "the order of authorization or approval" under which their communications were intercepted "is insufficient on its face." Id. § 2518(10)(a)(ii). Therefore, they are not entitled to suppression of evidence derived from the intercepted communications.

IV. Conclusion

For the foregoing reasons, Fernando Rivera Rodriguez's Motion to Suppress Evidence Derived from Electronic Surveillance Where Wiretap Order was Insufficient on its Face [#253], in which Isis Lugo-Guerrero and Jose Negron join, and Yeurys Tejeda's Motion to Suppress Evidence Derived from Wiretap Orders [#282] are DENIED.

IT IS SO ORDERED.

February 20, 2018

/s/ Indira Talwani
United States District Judge